ELSEVIER

Available online at www.sciencedirect.com
SCIENCE DIRECT®

Discrete Mathematics 268 (2003) 103–127

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Extremal weight enumerators and ultraspherical polynomials

Iwan Duursma*,[1]

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 W. Green Street (MC-382), Urbana, IL 61801-2915, USA

Received 6 August 2001; received in revised form 30 April 2002; accepted 13 May 2002

Abstract

We establish an upper bound for the minimum distance of a divisible code in terms of its dual distance. The bound generalizes the Mallows–Sloane bounds for self-dual codes. We obtain a linear recurrence for the distance distribution components of codes that attain the bound. From this we derive known conditions for the existence of extremal self-dual codes in a much simpler way. In the second half of the paper, we determine zeta functions for the codes that attain our new bound. Zeta functions for linear codes are defined in Duursma (Trans. Amer. Math. Soc. 351(9) (1999) 3609). Using properties of ultraspherical polynomials, we show that the zeta function of a quaternary extremal self-dual code has its zeros on the circle $|T|=q^{-1/2}$ in analogy with the zeta function of an algebraic curve.

MSC: 94B65; 33C45; 11R58

Keywords: Extremal code; Divisible code; Minimum distance bound; Riemann hypothesis; Gegenbauer polynomial

1. Introduction

A linear code of length n over a finite field F_q of q elements is a subspace of n-letter words over F_q. The weight distribution of a linear code is the vector $(A_0=1,A_1,\ldots,A_n)$, where A_i gives the number of words in the code with i coordinates different from 0.

* Tel.: +1-217-265-0677; fax: +1-217-333-9576.
E-mail address: duursma@math.uiuc.edu (I. Duursma).
URL: http://www.math.uiuc.edu/∼duursma
[1] Supported by NSF Grant DMS-0099761.

0012-365X/03/$ - see front matter
PII: S0012-365X(02)00683-0

The smallest nonzero value of i such that $A_i > 0$ is called the minimum distance of the code and is denoted by d. The weight distribution may be represented by a polynomial $A(x, y) = \sum_i A_i x^{n-i} y^i$ called the weight enumerator. We consider A as a function of the row vector (x, y). So that the result of a linear substitution can be written as $A((x, y)\sigma)$. A code is said to be formally self-dual if the weight enumerator is invariant under the involution

$$\sigma = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}.$$

A self-dual code is extremal if it meets one of the Mallows–Sloane upper bounds for the minimum distance. We briefly recall these bounds and describe our results for extremal weight enumerators.

1.1. Extremal weight enumerators

A linear code over the field F_q of q elements has as main parameters its length n, dimension k, and minimum distance d. The dual code has length n, dimension $n-k$, and minimum distance $d^\perp$. The Singleton bound gives

$$k + d \leqslant n + 1.$$

Codes that meet the bound with equality are called maximum distance separable (MDS). The dual of an MDS code is again MDS. And a code is MDS if and only if

$$\text{(MDS)} \quad d + d^\perp = n + 2.$$

A code is said to be divisible by c if the Hamming distance between any two words is divisible by c. A binary code is said to be self-complementary if it contains the all-one word. We will prove our results for codes that satisfy, for a given c, one of the following assumptions:

(Type 1) C is divisible by c,
(Type 2) C is divisible by c and both C and its dual are binary self-complementary.

In Theorem 3, we obtain the following bounds:

$$\text{(Type 1)} \quad d + cd^\perp \leqslant n + c(c+1),$$
$$\text{(Type 2)} \quad 2d + cd^\perp \leqslant n + c(c+2).$$

We call a code or weight enumerator *extremal divisible* if the bound is attained. Upon restriction to self-dual codes the bounds become (using that $cx \leqslant y$ improves to $cx \leqslant c\lfloor y/c \rfloor$ when x is an integer)

$$\text{(Type 1)} \quad d \leqslant c\lfloor n/c(c+1) \rfloor + c \quad \text{(self-dual)},$$
$$\text{(Type 2)} \quad d \leqslant c\lfloor n/c(c+2) \rfloor + c \quad \text{(self-dual)}.$$

The Gleason–Prange theorem [10,11] classifies the nontrivial self-dual divisible codes among four cases:

$$\begin{aligned}&\text{(Type I)} && (q,c)=(2,2)\ 2|n,\\ &\text{(Type II)} && (q,c)=(2,4)\ 8|n,\\ &\text{(Type III)} && (q,c)=(3,3)\ 4|n,\\ &\text{(Type IV)} && (q,c)=(4,2)\ 2|n.\end{aligned}$$

In each case, the parameters are bounded by the Mallows–Sloane upper bounds [8]

$$\begin{aligned}&\text{(Type I)} && d\leqslant 2\lfloor n/8\rfloor+2,\\ &\text{(Type II)} && d\leqslant 4\lfloor n/24\rfloor+4,\\ &\text{(Type III)} && d\leqslant 3\lfloor n/12\rfloor+3,\\ &\text{(Type IV)} && d\leqslant 2\lfloor n/6\rfloor+2.\end{aligned}\tag{1}$$

Thus, the bounds for Types 1 and 2 codes generalize the Mallows–Sloane bounds. Rains [9] proved that Type I codes satisfy the bound for Type II codes, except when $n\equiv 22\,(\mathrm{mod}\,24)$, in which case $d\leqslant 4\lfloor n/24\rfloor+6$. A code or weight enumerator is called extremal if it attains one of the Mallows–Sloane bounds. We will call such codes *extremal self-dual*. We formulate our results first for divisible and extremal divisible codes. When the codelength is not divisible by $c(c+1)$ or $c(c+2)$ an extremal self-dual code is not extremal divisible. But the results extend without difficulty to all extremal self-dual codes. Extremal divisible codes that are not self-dual include all MDS codes (that are of Type 1 with $c=1$) and the binary first-order Reed–Muller codes (that have $d=n/2$ and $d^{\perp}=4$) and their dual codes (that both attain the bound for Type 2 codes with $c=2$).

Theorem 3 shows that the weight enumerator of an extremal divisible code is completely determined by the parameters n and d of the code. Theorem 12 gives the extension to all extremal self-dual codes. For extremal self-dual codes uniqueness of the weight enumerator is known but the expressions that we obtain are much simpler. In particular, our expressions immediately reveal the sign of A_{d+c}/A_d (Theorems 4 and 12), reducing the vast amount of work that is required when using the hereto known results. Our expressions yield linear recurrence relations for the coefficients of an extremal divisible weight enumerator. They are given explicitly with a direct proof in Theorem 6. In all cases, the computation of an extremal weight enumerator reduces to a trivial exercise that routinely produces all extremal self-dual weight enumerators that are known to have positive coefficients.

1.2. Zeta functions

The problem that motivated this paper is to find upper bounds for the minimum distance of self-dual codes through their weight enumerator: that is to find for given n and q, the largest possible d such that a σ-invariant polynomial $A(x,y)$ exists with nonnegative coefficients and such that $y^d|(A(x,y)-x^n)$. This is essentially a linear programming problem. It is an open problem to determine a sharp upper bound for the

relative distance $\limsup d/n$ as n goes to infinity. Under an unproven assumption we can prove that $\limsup d/n \leqslant 1/2 - 1/(2\sqrt{q})$ [4]. The assumption is formulated in terms of the *zeta function of a linear code*. The latter is defined in [3] as the function

$$Z(T) = \frac{P(T)}{(1-T)(1-qT)}$$

such that the power series development around $T = 0$ of

$$Z(T)(y(1-T)+xT)^n$$

has as coefficient at T^{n-d}

$$(A(x,y) - x^n)/(q-1).$$

The function shows similarities with the zeta function of an algebraic curve and further properties were derived in [4,5]. We observed that in many cases but not always the zeta function of a formally self-dual linear code over a field of q elements has its zeros $T = q^{-s}$ on the circle $|T| = q^{-1/2}$ (which we call the Riemann hypothesis property or RH property). In [4], it is shown that for an infinite family of formally self-dual codes of increasing length that have the RH property and that satisfy an additional positivity criterion, the relative minimum distance satisfies $\limsup d/n \leqslant 1/2 - 1/(2\sqrt{q})$ as $n \to \infty$. We believe that if the minimum distance d is attained by some self-dual code of length n, then there exists a self-dual weight enumerator with the same d and n that verifies the RH property. If true, the value $1/2 - 1/(2\sqrt{q})$ can be used as an upper bound for general self-dual codes. Thus we are particularly interested in the RH property for extremal self-dual weight enumerators, that are uniquely determined by their parameters n and d.

Implicit expressions for extremal self-dual weight enumerators appear in the literature but we could not obtain the zeta functions from them. Thus, we give our own expressions in Theorem 12 that have a short proof and from which we easily obtain various properties of extremal self-dual weight enumerators. In Theorem 19, we consider for each family the transformation of the weight enumerator into a zeta function. To analyze the zeros of the zeta functions we give expressions for them in terms of ultraspherical polynomials using Theorem 20. We find that the zeta function of an extremal type IV code of length $n = 3m + 3$ and minimum distance $d = m + 3$, for m odd, has a complex zero $T = q^{-1/2}e^{2i\theta}$ only if $\cos\theta$ is a zero of the ultraspherical polynomial $C_m^{m+1}(x)$.

1.3. Ultraspherical polynomials

For any $\lambda > -1/2$, the ultraspherical or Gegenbauer polynomials $\{C_n^\lambda(x)\}$ of degree n are defined as the family of orthogonal polynomials for the weight function $(1-x^2)^{\lambda-1/2}$ on the interval $[-1,1]$ normalized such that

$$C_n^\lambda(1) = \binom{n+2\lambda+1}{n} = \frac{\Gamma(n+2\lambda+2)}{\Gamma(2\lambda+2)n!}.$$

Upto normalization they are a special case of Jacobi polynomials,

$$C_n^\lambda(x) = \frac{(2\lambda)_n}{(\lambda+1/2)_n} P_n^{(\lambda-1/2,\lambda-1/2)},$$

where we follow the notation $(a)_n = a(a+1)\cdots(a+n-1)$.

Among the properties that we will use are a classical interpretation of the zeros of a Jacobi polynomial (going back to Stieltjes) and an expansion of the ultraspherical polynomial as cosine polynomial. These and other properties of ultraspherical polynomials, such as their generating function, recurrence relation, differential equation and others, can be found in [12]. When there is a conflict with the code length n, we will denote the degree of an ultraspherical polynomial by v and the code length by n.

The Jacobi polynomial $P_n^{(2p-1,2q-1)}(x)$, for $p,q>0$, has n real zeros in the interval $[-1,1]$ that correspond to the equilibrium positions of n unit charges placed in the interval $[-1,1]$ together with two charges p and q fixed at the end points $x=-1$ and 1.

A polynomial $R(T)=\sum_{i=0}^{v} r_i T^i$ is self-reciprocal if $r_i = r_{v-i}$. After we transform a weight enumerator into a zeta function, we obtain self-reciprocal polynomials $R(T)$ that satisfy for some $\lambda > -\frac{1}{2}$,

$$\sum_{i=0}^{v} r_i \binom{v+2\lambda-2}{\lambda-1+i} T^i = (1+T)^v.$$

Their zeros can be located using ultraspherical polynomials. The ultraspherical polynomial $C_n^\lambda(x)$ has cosine polynomial

$$C_n^\lambda(\cos\theta) = \sum_{\substack{0\leqslant k,\ell\leqslant n \\ k+\ell=n}} \binom{\lambda+k}{k}\binom{\lambda+\ell}{\ell} \cos(k-\ell)\theta.$$

Moreover, it is easily derived that, for $T=\mathrm{e}^{\mathrm{i}\theta}$,

$$\frac{R(T^2)}{T^v} = \frac{v!(\lambda-1)!(\lambda-1)!}{(v+2\lambda-2)!} C_v^\lambda(\cos\theta).$$

Thus all zeros of $R(T)$ lie on the unit circle. For $\lambda=1$, $R(T)=1+T+\cdots+T^v$ and the zeros of $R(T)$ together with $T=1$ are equally distributed on the unit circle. As λ increases, the interpretation of the zeros of C_n^λ shows that we should expect the zeros to move along the circle away from $T=1$ and towards $T=-1$.

2. Divisible weight enumerators

For a homogeneous polynomial p over the complex numbers, let $p(D)$ be the differential operator defined by replacing each occurrence of x_j in p by $\partial/\partial x_j$. For a code with homogeneous weight enumerator $A(x,y)$, we seek pairs of polynomials $a(x,y)$ and $p(x,y)$ such that

$$a(x,y) \mid p(x,y)(D)A(x,y). \tag{2}$$

A linear code with minimum distance d has

$$A(x,y)=x^n+A_dx^{n-d}y^d+\cdots+A_ny^n.$$

Our first relation of the form (2) is

$$y^{d-1}\mid y(D)A(x,y). \tag{3}$$

Other relations follow from trivial manipulations, involving linear transformations of the form

$$(u\quad v)=(x\quad y)\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

with matching transformation of differential operators

$$(\partial/\partial_x\quad \partial/\partial_y)=(\partial/\partial_u\quad \partial/\partial_v)\begin{pmatrix}a & c\\ b & d\end{pmatrix}.$$

It is easy to see that, for a linear transformation $(u,v)=(x,y)\sigma$ and for any two homogeneous polynomials $A(x,y)$ and $p(x,y)$,

$$A((x,y)\sigma)=A(u,v)\quad\text{and}\quad p(x,y)(D)=p((u,v)\sigma^T)(D).$$

Lemma 1. *For a linear transformation* $(u,v)=(x,y)\sigma$,

$$p((u,v)\sigma^T)(D)A(u,v)=p(x,y)(D)A((x,y)\sigma).$$

A binary self-complementary code has $A(x,y)=A(y,x)$, and with

$$(u\quad v)=(x\quad y)\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},$$

$$x^{d-1}=v^{d-1}\mid v(D)A(u,v)=x(D)A(x,y),$$

which together with (3) yields

$$(xy)^{d-1}\mid xy(D)A(x,y). \tag{4}$$

Let σ be given by the MacWilliams transform,

$$(u\quad v)=(x\quad y)\begin{pmatrix}1 & 1\\ q-1 & -1\end{pmatrix}.$$

Then, for a code with dual distance $d^\perp$,

$$(x-y)^{d^\perp-1}=qv^{d^\perp-1}\mid qv(D)A^\perp(u,v)=((q-1)x-y)(D)A(x,y)q^{n-k}.$$

A divisible code has $A(x,y)=A(x,\zeta y)$ for all ζ with $\zeta^c=1$. Another application of Lemma 1, now with

$$(u\quad v)=(x\quad y)\begin{pmatrix}1 & 0\\ 0 & \zeta\end{pmatrix}$$

gives, for all ζ with $\zeta^c = 1$,

$$(x - \zeta y)^{d^\perp - 1} = (u - v)^{d^\perp - 1} \mid ((q-1)u - v)(D)A(u,v)$$
$$= ((q-1)x - \zeta y)(D)A(x,y),$$

so that

$$(x^c - y^c)^{d^\perp - c} \mid ((q-1)^c x^c - y^c)(D)A(x,y). \tag{5}$$

The latter can be sharpened for even binary codes. In that case the dual code $C^\perp$ is self-complementary and we can use (4) instead of (3). For all ζ with $\zeta^c = 1$,

$$(x^2 - \zeta^2 y^2)^{d^\perp - 1} = (u^2 - v^2)^{d^\perp - 1} \mid (u^2 - v^2)(D)A(u,v) = (x^2 - \zeta^2 y^2)(D)A(x,y),$$

so that

$$(x^c - y^c)^{d^\perp - c + 1} \mid (x^c - y^c)(D)A(x,y). \tag{6}$$

Lemma 2. *For a divisible code with weight enumerator $A(x,y)$, let*

$$\text{(Type 1)} \quad a(x,y) = y^{d-c-1}(x^c - y^c)^{d^\perp - c - 1} \quad p(x,y) = y(y^c - (q-1)^c x^c),$$
$$\text{(Type 2)} \quad a(x,y) = (xy)^{d-c-1}(x^c - y^c)^{d^\perp - c - 1} \quad p(x,y) = xy(y^c - x^c).$$

Then $a(x,y) \mid p(x,y)(D)A(x,y)$.

Proof. For the first claim, combine (3) and (5). For the second claim, combine (4) and (6). □

Theorem 3. *Let C be a code of length n with minimum distance d and dual distance $d^\perp$. Let $A(x,y)$ be the weight enumerator of C and assume C is divisible by c, then*

$$\text{(Type 1)} \quad d + cd^\perp \leqslant n + c(c+1),$$
$$\text{(Type 2)} \quad 2d + cd^\perp \leqslant n + c(c+2)$$

with equality if and only if

$$\text{(Type 1)} \quad p(x,y)(D)A(x,y) = (d-c)_{c+1} A_d a(x,y),$$
$$\text{(Type 2)} \quad p(x,y)(D)A(x,y) = (n-d)(d-c)_{c+1} A_d a(x,y),$$

where $a(x,y)$ and $p(x,y)$ are given by Lemma 2.

Proof. The bounds follow immediately from the lemma. They are met if and only if $p(x,y)(D)A(x,y)$ is equal to $a(x,y)$ up to a constant. And the constants follow by comparing coefficients at the smallest powers of y. □

The (Type 1) case of the theorem applies to MDS codes with $c = 1$. The weight enumerators in the theorem are uniquely determined as the solution to the given differential equation with minimum distance d.

The theorem has several uses. As we showed in Section 1.1, the Mallows–Sloane bounds follow from Theorem 3 and deriving them in this way does not require the computation of a ring of invariants. The theorem gives a precise description of extremal weight enumerators. On the one hand this description makes it straightforward to determine the sign of the coefficient A_{d+c} of an extremal weight enumerator. On the other hand the description allows us to establish the zeta function of an extremal weight enumerator (our original purpose).

2.1. Positive weight enumerators

For the weight enumerators in Theorem 3 to be realizable by a code, the coefficients must be nonnegative.

Theorem 4. *For a divisible code that attains the bound in Theorem 3, $A_{d+c}/A_d \geqslant 0$ if and only if*

$$\text{(Type 1)} \quad (d^\perp - c - 1)(d-c)_c \leqslant (q-1)^c (n-d-c+1)_c,$$
$$\text{(Type 2)} \quad (d^\perp - c - 1)(d-c)_c \leqslant (n-d-c)_c.$$

Proof. For the first case, the second part of Theorem 3 gives

$$y(y^c - (q-1)^c x^c)(D)A(x,y) = (d-c)_{c+1} A_d y^{d-c-1} (y^c - x^c)^{d^\perp - c - 1}.$$

And the claim follows after comparing the coefficients at $x^{n-d-c} y^{d-1}$,

$$(d)_{c+1} A_{d+c} - (q-1)^c (n-d-c+1)_c d A_d = -(d-c)_{c+1} A_d (d^\perp - c - 1).$$

For the other case, Theorem 3 gives

$$xy(y^c - x^c)(D)A(x,y) = (d-c)_{c+1}(n-d) A_d (xy)^{d-c-1} (x^c - y^c)^{d^\perp - c - 1}.$$

And comparing coefficients at $x^{n-d-c-1} y^{d-1}$ yields

$$(d)_{c+1}(n-d-c) A_{d+c} - (n-d-c)_{c+1} d A_d$$
$$= -(d-c)_{c+1}(n-d) A_d (d^\perp - c - 1). \qquad \square$$

After replacing $d^\perp$ by an expression in n and d the bounds give

$$\text{(Type 1)} \quad (n-d) \leqslant c(q-1)^c (n-d-c+1)_c / (d-c)_c,$$
$$\text{(Type 2)} \quad (n-2d+c) \leqslant c(n-d-c)_c / (d-c)_c.$$

It follows that for a family of codes with $d/n > \varepsilon > 0$, the expressions $n-d$ or $n-2d+c$ are bounded. Any such family of unbounded length must have $\liminf d/n \geqslant 1$ or $\liminf d/n \geqslant 1/2$, respectively, as $n \to \infty$. Examples are (1) Repetition codes with $n = d$, and (2) First-order Reed–Muller codes with $n = 2d$. In each case, the dual family is unbounded with $\lim d/n = 0$, as $n \to \infty$.

2.2. Recurrence relations

From the expressions in Theorem 3, the coefficients $A_d, A_{d+c}, A_{d+2c}, \ldots$, of an extremal weight enumerator can be computed recursively provided the initial coefficient A_d is known. In this section, we derive the recurrence relations in a different way. We first give the relations for MDS weight enumerators. Then we relate the relations for extremal divisible codes to those of MDS codes.

Let $M(x,y)=M_{n,d}(x,y)$ be the weight enumerator of an MDS code of length n and minimum distance d. Let $m_w = M_w/(q-1)\binom{n}{w}$.

Lemma 5.

$$m_w - (q-1)m_{w-1} = (-1)^{w-d}\binom{w-2}{d-2}.$$

Proof. It is not hard to verify this using known expressions for M_w [7]. It is also straightforward using the generating function given in [4].

We include a proof of the lemma based on Theorem 3. It gives

$$y(y-(q-1)x)(D)M(x,y) = d(d-1)M_d y^{d-2}(x-y)^{d^\perp-2}$$

or, using $M_d = (q-1)\binom{n}{d}$,

$$\frac{1}{n(n-1)(q-1)}\, y(y-(q-1)x)(D)M(x,y) = \binom{n-2}{d-2} y^{d-2}(x-y)^{n-d}.$$

Comparison of the coefficient at $y^{w-2}x^{n-w}$ gives

$$\frac{1}{n(n-1)(q-1)}\,(w(w-1)M_w - (q-1)(w-1)(n-w+1)M_{w-1})$$

$$= \binom{n-2}{d-2}(-1)^{w-d}\binom{n-d}{w-d}.$$

Rewriting in terms of m_w gives

$$\binom{n-2}{w-2}(m_w-(q-1)m_{w-1}) = \binom{n-2}{d-2}(-1)^{w-d}\binom{n-d}{n-w},$$

which simplifies to give the required result. Next, we consider the weight enumerator $A(x,y)=A_{N,D}(x,y)$ of an extremal divisible code of length N and minimum distance D. □

Theorem 6. *For an MDS weight enumerator $M(x,y)=M_{n,d}(x,y)$, let*

$$(\nabla M)(x,y) = \frac{1}{n(q-1)}((q-1)x-y)(D)M(x,y).$$

For a divisible code with weight enumerator $A(x,y)=A_{N,D}(x,y)$ *let*

$$(\nabla A)(x,y)=\frac{1}{(n-c+1)_c(q-1)^c}\left((q-1)^c x^c-y^c\right)(D)A(x,y)$$

For an extremal divisible code, and for n *and* d *such that* $d=D/c$, $d^\perp=D^\perp-c+1$, $n=d+d^\perp-2$,

$$\text{(Type 1)}\quad (\nabla A)(x,y)=(\nabla M)(x^c,y^c),$$
$$\text{(Type 2)}\quad (\nabla A)(x,y)=x^{D-c}(\nabla M)(x^c,y^c)-y^{D-c}(\nabla M)(y^c,x^c).$$

Proof. Note that in the first case, $D+cD^\perp=N+c(c+1)$, so that $n=d+d^\perp-2=N/c$. While in the second case, $D+cD^\perp=(N-D+c)+c(c+1)$, and $n=(N-D+c)/c$. For (Type 1), $(\nabla A)(x,y)$ is uniquely determined by

$$(x^c-y^c)^{D^\perp-c}\mid \nabla A=x^{N-c}+y^{D-c}F_{D^\perp-c-1}(x^c,y^c)$$

for a homogeneous polynomial $F_{D^\perp-c-1}$ of degree $D^\perp-c-1$. On the other hand, $(\nabla M)(x,y)$ is uniquely determined by

$$(x-y)^{d^\perp-1}\mid \nabla M=x^{n-1}+y^{d-1}f_{d^\perp-2}(x,y) \tag{7}$$

for a homogeneous polynomial $f_{d^\perp-2}$ of degree $d^\perp-2$. So that $F_{D^\perp-c-1}=f_{d^\perp-2}$. In the second case, $(\nabla A)(x,y)$ is uniquely determined by

$$(x^c-y^c)^{D^\perp-c}\mid \nabla A=x^{N-c}-y^{N-c}+(xy)^{D-c}G_{D^\perp-c-1}(x^c,y^c).$$

From (7), $(\nabla M)(x,y)$ is uniquely determined by

$$\begin{aligned}&(x-y)^{d^\perp-1}\mid x^{d-1}\nabla M_d(x,y)-y^{d-1}\nabla M_d(y,x)\\ &\quad=x^{n+d-2}-y^{n+d-2}+(xy)^{d-1}(f_{d^\perp-2}(x,y)-f_{d^\perp-2}(y,x)).\end{aligned}$$

So that $G_{D^\perp-c-1}(x,y)=f_{d^\perp-2}(x,y)-f_{d^\perp-2}(y,x)$. □

For an extremal divisible code, the theorem yields both a recurrence relation for the coefficients $A_D, A_{D+c},\ldots$, and an expression for the initial coefficient A_D. For the recurrence relation it is convenient to introduce normalized coefficients. Let m_w and μ_w denote the normalized coefficients:

$$m_w=M_w/(q-1)\binom{n}{w},\quad \mu_w=M_w/(q-1)^w\binom{n}{w}.$$

Let a_W and α_W denote the normalized coefficients

$$a_W=A_W/(q-1)\binom{N}{W},\quad \alpha_W=A_w/(q-1)^W\binom{N}{W}.$$

Corollary 7. *For an extremal divisible code, and for* $W = cw$,

$$\text{(Type 1)} \quad \binom{N-c}{W}(q-1)^W(\alpha_W - \alpha_{W+c}) = \binom{n-1}{w}(q-1)^w(\mu_w - \mu_{w+1}),$$

$$\text{(Type 2)} \quad \binom{N-c}{W}(a_W - a_{W+c})$$

$$= \binom{n-1}{w}(m_w - m_{w+1})$$

$$- \binom{n-1}{n+d-2-w}(m_{n+d-2-w} - m_{n+d-1-w}).$$

Proof. Compare the coefficients at $x^{N-W-c}y^W$ in the equalities of Theorem 6 that relate (∇A) and (∇M),

$$\frac{(N-W-c+1)_c}{(N-c+1)_c}A_W - \frac{1}{(q-1)^c}\frac{(W+1)_c}{(N-c+1)_c}A_{W+c}$$

$$= \frac{n-w}{n}M_w - \frac{w+1}{n}\frac{1}{q-1}M_{w+1}.$$

For the second case, the right-hand side is replaced with

$$\left(\frac{n-w}{n}M_w - \frac{w+1}{n}M_{w+1}\right)$$

$$- \left(\frac{w-d+2}{n}M_{n+d-2-w} - \frac{n+d-1-w}{n}M_{n+d-1-w}\right). \qquad \square$$

Corollary 8. *For an extremal divisible code*,

$$\text{(Type 1)} \quad A_D = (q-1)^c\binom{N/c-1}{D/c-1}(N-c+1)_c/(D-c+1)_c,$$

$$\text{(Type 2)} \quad A_D = \binom{N/c-D/c-1}{D/c-2}(N-c)_{c+1}/(D-c)_{c+1}.$$

Proof. The relations in the previous corollary have left-hand side, for $W = D-c$,

$$\binom{N-c}{D-c}(q-1)^{D-c}\left(-A_D/(q-1)^D\binom{N}{D}\right),$$

while Lemma 5 gives for the right-hand side

$$-\binom{n-1}{d-1} \quad \text{or} \quad -\binom{n-1}{d-1} + (-1)^{n-d}\binom{n-2}{d-2}$$

for the cases (Type 1) and (Type 2), respectively. Replacing n and d with expressions in N and D proves the case (Type 1). To complete the case (Type 2), note that $n-d=d^{\perp}-2=D^{\perp}-c-1\equiv 1 \pmod 2$ and use

$$\binom{n-1}{d-1}+\binom{n-2}{d-2}=\frac{N-c}{D-c}\binom{n-2}{d-2}. \qquad \square$$

3. Self-dual weight enumerators

Let σ be given by the MacWilliams transform

$$\sigma=\begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}.$$

Let $\gamma(x,y)$ and $p(x,y)$ be as follows:

$$\begin{array}{ll} \text{(Type 1)} & \gamma(x,y)=y(y^c-x^c) \quad p(x,y)=y(y^c-(q-1)^c x^c), \\ \text{(Type 2)} & \gamma(x,y)=xy(y^c-x^c) \quad p(x,y)=xy(y^c-x^c). \end{array}$$

So that $p(x,y)=\gamma((x,y)\rho)$, for

$$\rho=\begin{pmatrix} q-1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Lemma 9.

$$\gamma((x,y)\sigma)=\lambda\gamma(x,y) \;\Leftrightarrow\; p((x,y)\sigma^t)=\lambda p(x,y).$$

Proof. $\sigma^t\rho=\rho\sigma$. $\square$

Lemma 10. *$\gamma((x,y)\sigma)=\lambda\gamma(x,y)$ if and only if one of the following*:

$$\begin{array}{ll} (q,c)=(q,1) & (\lambda=q), \\ (q,c)=(2,2) & (\lambda=4), \\ (q,c)=(2,4) & (\lambda=8), \\ (q,c)=(3,3) & (\lambda=9), \\ (q,c)=(4,2) & (\lambda=8). \end{array}$$

Proof. Assume $c>1$ and let $y\neq 0,1$ be a zero of $\gamma(1,y)$. Then $q-2\leqslant|1+(q-1)y| =|1-y|\leqslant 2$ or $q\leqslant 4$. For $q=2,3,4$, the only possibilities for c are those listed. $\square$

It is not a surprise that the only cases for which γ is invariant are the cases given by the Gleason–Prange theorem. The proof of that theorem, as given in [11], derives first as a necessary condition that γ is invariant (to guarantee finiteness of the Galois group of the weight enumerator). The proof in [11] then continues to find restrictions on c. In the lemma we first restrict q.

Lemma 11. *For a self-dual divisible weight enumerator $A(x,y)$, let $a(x,y)=\gamma(x,y)^{d-c-1}$ and $p(x,y)$ be as in Lemma 2. Let $\tilde{a}(x,y)$ be defined as the cofactor in*

$$a(x,y) \mid p(x,y)(D)A(x,y).$$

Then $\tilde{a}(x,y)$ is divisible by c (that is to say y occurs only to the power y^c) and is invariant under the MacWilliams transform σ.

Proof. Obviously $\tilde{a}(x,y)$ is divisible. Since $p(x,y)$ is invariant under σ^t,

$$a(u,v)\tilde{a}(u,v) \mid p(u,v)(D)A(u,v)$$

if and only if

$$a(u,v)\tilde{a}(u,v) \mid p((u,v)\sigma^t)(D)A(u,v).$$

As in Lemma 1 with $(u,v)=(x,y)\sigma$ this gives

$$a((x,y)\sigma)\tilde{a}((x,y)\sigma) \mid p(x,y)(D)A((x,y)\sigma).$$

Now use that $a(x,y)$ and $A(x,y)$ are both invariant under σ. □

Results as in Theorem 4 can be obtained similarly for all extremal self-dual codes. The parameters n and d to consider are those that attain the Mallows–Sloane bounds (1).

$$\begin{aligned}
&\text{(I)} && d=2\lfloor n/8\rfloor+2 \quad \text{or} \quad n=4(d-2)+2v, \quad v=0,1,2,3,\\
&\text{(II)} && d=4\lfloor n/24\rfloor+4 \quad \text{or} \quad n=6(d-4)+8v, \quad v=0,1,2,\\
&\text{(III)} && d=3\lfloor n/12\rfloor+3 \quad \text{or} \quad n=4(d-3)+4v, \quad v=0,1,2,\\
&\text{(IV)} && d=2\lfloor n/6\rfloor+2 \quad \text{or} \quad n=3(d-2)+2v, \quad v=0,1,2.
\end{aligned}$$

Theorem 12. *Extremal weight enumerators of type* (I)–(IV) *satisfy*

$$\begin{aligned}
&\text{(I)} && (xy^3-x^3y)(D)A(x,y)=(d-2)_3(n-d)A_d(x^3y-xy^3)^{d-3}(x^2+y^2)^v,\\
&\text{(II)} && (xy^5-x^5y)(D)A(x,y)\\
&&& \quad =(d-4)_5(n-d)A_d(x^5y-xy^5)^{d-5}(x^8+14x^4y^4+y^8)^v,\\
&\text{(III)} && (y^4-8x^3y)(D)A(x,y)=(d-3)_4A_d(y^4-x^3y)^{d-4}(x^4+9xy^3)^v,\\
&\text{(IV)} && (y^3-9x^2y)(D)A(x,y)=(d-2)_3A_d(y^3-x^2y)^{d-3}(x^2+3y^2)^v.
\end{aligned}$$

In each case, $A_{d+c}/A_d \geqslant 0$ if and only if

$$\begin{aligned}
&\text{(I)} && (d-3-v)(d-2)_2 \leqslant (n-d-2)_2,\\
&\text{(II)} && (d-5-14v)(d-4)_4 \leqslant (n-d-4)_4,\\
&\text{(III)} && (d-4-8v)(d-3)_3 \leqslant 8(n-d-2)_3,\\
&\text{(IV)} && (d-3-3v)(d-2)_2 \leqslant 9(n-d-1)_2.
\end{aligned}$$

Proof. The expression $p(x,y)(D)A(x,y)=a(x,y)\tilde{a}(x,y)$ is determined up to the cofactor $\tilde{a}(x,y)$ of small degree. The cofactor is divisible and invariant under the MacWilliams transform. In each case, because of the small degree, this determines the cofactor uniquely. The inequalities and their proof are similar to Theorem 4 with an extra contribution for $v\neq 0$. □

The numerical results obtained with the bounds agree with those obtained previously in [14]. Our proof is considerably shorter.

Corollary 13 (Zhang [14]). *Extremal weight enumerators of type* (I)–(IV) *have* $A_{d+c}/A_d \geqslant 0$ *if and only if*

	$(v=0)$		$(v=1)$		$(v=2)$		$(v=3)$	
(Type I)	$n\leqslant 24$	$(d\leqslant 8)$	$n\leqslant 34$	$(d\leqslant 10)$	$n\leqslant 44$	$(d\leqslant 12)$	$n\leqslant 54$	$(d\leqslant 14)$,
(Type II)	$n\leqslant 3672$	$(d\leqslant 616)$	$n\leqslant 3800$	$(d\leqslant 636)$	$n\leqslant 3928$	$(d\leqslant 656)$,		
(Type III)	$n\leqslant 828$	$(d\leqslant 210)$	$n\leqslant 892$	$(d\leqslant 225)$	$n\leqslant 932$	$(d\leqslant 234)$,		
(Type IV)	$n\leqslant 96$	$(d\leqslant 34)$	$n\leqslant 116$	$(d\leqslant 40)$	$n\leqslant 130$	$(d\leqslant 44)$.		

3.1. Binomial moments

Let C be a code of length n. For a subset S of $\{1,2,\ldots,n\}$, let A_S be the number of words in C that are zero on S. Define

$$B(x,y)=\sum_{i=0}^{n} B_i x^{n-i}y^i=\sum_{S\subset\{1,\ldots,n\}} A_S x^{|S|}y^{n-|S|}. \tag{8}$$

The coefficients B_i are called the binomial moments of the code. A codeword of C contributes to B_i for each subset S of size $n-i$ on which the word is zero. For a word of weight $j\leqslant i$ there are $\binom{n-j}{n-i}$ such subsets. Thus

$$B(x,y)=\sum_{j=0}^{n} A_j\left(\sum_{i=j}^{n}\binom{n-j}{n-i}x^{n-i}y^{i-j}\right)y^j=A(x+y,y).$$

From $A^{\perp}(x,y)=A(x+(q-1)y,x-y)/q^k$ and $B^{\perp}(x,y)=A^{\perp}(x+y,y)$,

$$B^{\perp}(x,y)=A(x+qy,x)/q^k=B(qy,x)/q^k$$

and duality for $B(x,y)$ is particularly straightforward (admittedly, it would be easy to prove the relation between $B(x,y)$ and $B^{\perp}(x,y)$ directly and derive from it the MacWilliams duality for $A(x,y)$).

Theorem 14. *For a code with weight enumerator* $A(x,y)$, *let* $B(x,y)=A(x+y,y)$. *Assume the code has minimum distance* $d\geqslant 2$ *and dual minimum distance* $d^{\perp}\geqslant 2$.

Then

$$y^{d-2}x^{d^\perp-2} \mid (y-x)(y-qx)(D)B(x,y).$$

Moreover, in each of the following special cases $b(x,y) \mid q(x,y)(D)B(x,y)$

	$b(x,y)$	$q(x,y)$
(Type III)	$(xy)^{d-4}(x^2+3xy+3y^2)^{d-4}$	$(y-x)(y-3x)(y^2+3x^2)$
(Type IV)	$(xy)^{d-3}(x+2y)^{d-3}$	$(y-x)(y-4x)(y+2x)$
(Type I)	$(xy)^{d-3}(x^2+3xy+2y^2)^{d-3}$	$(y-x)(y-2x)xy$
(Type II)	$(xy)^{d-5}(x^4+5x^3y$ $+10x^2y^2+10xy^3+4y^4)^{d-5}$	$(y-x)(y-2x)xy(y^2-2xy+2x^2)$

Proof. We transform the relation $a(x,y) \mid p(x,y)(D)A(x,y)$ of Lemma 2. Using Lemma 1 with

$$(u \quad v) = (x \quad y)\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

we find that

$$q(x,y)(D)B(x,y) = q(x,y)(D)A(x+y,y) = q(u,u+v)(D)A(u,v).$$

And for $p(u,v) = q(u,u+v)$ this last expression is divisible by $a(u,v)$. In other words, the claim holds with $q(x,y) = p(x,y-x)$ and $b(x,y) = a(x+y,y)$. □

Both operators are useful. From the action of $p(x,y)(D)$ on $A(x,y)$ it is immediate that for a divisible weight enumerator $A(x,y)$, the result $p(x,y)(D)A(x,y)$ has only terms $x^i y^j$ with $j \equiv -1 \pmod{c}$. From the action of $q(x,y)(D)$ on $B(x,y)$ it follows that in all cases an invariant polynomial $B(x,y)$ is mapped to another invariant polynomial.

In [4], we use operators P and S that represent puncturing and averaging and shortening and averaging, respectively. They are defined as

$$S = \left(\frac{\partial}{\partial_x}\right)\Big/ n, \quad P = \left(\frac{\partial}{\partial_x} + \frac{\partial}{\partial_y}\right)\Big/ n.$$

So that if we express $p(x,y)(D)A(x,y)$ in terms of P and S, we obtain $q(nS, nP)$ $A(x,y)$.

4. Weight enumerators and zeta functions

Let C be a linear code of length n and minimum distance d over the finite field of q elements with weight enumerator $A(x,y)$. Let $d^\perp$ be the minimum distance of the dual code $C^\perp$. To avoid dealing with degenerate cases we will assume throughout that both

C and its dual $C^\perp$ have effective length n, or equivalently, that both have minimum distance at least two.

Under these assumptions, Theorem 14 gives

$$y^{d-2}x^{d^\perp-2} \mid (y-x)(y-qx)(D)B(x,y).$$

The right-hand side is of degree $n-2$ and determines the weight enumerator. On the other hand, after division a polynomial of degree only $(n-2)-(d-2)-(d^\perp-2)=n+2-d-d^\perp$ remains from which the weight enumerator can be determined. Thus, weight enumerators contain a lot of redundant coefficients and can be represented in different forms. Zeta functions provide another way to describe weight enumerators through fewer coefficients. They are defined in [3] as rational functions $Z(T)$ such that $Z(T)(y+(x-y)T)^n$ is a generating function for the weight enumerator. Let $[T^d]g(T)$ stand for the coefficient of T^d in the series expansion of $g(T)$ around $T=0$.

Definition 15 (Duursma [3]). For a q-ary linear code of length n and minimum distance d with weight enumerator $A(x,y)$, the *zeta polynomial*

$$P(T)=p_0+p_1T+\cdots+p_rT^r$$

is defined as the unique polynomial of degree at most $n-d$ such that

$$[T^{n-d}]\frac{P(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n=\frac{A(x,y)-x^n}{q-1}. \tag{9}$$

The quotient $Z(T)=P(T)/((1-T)(1-qT))$ is called the *zeta function* of the linear code.

Note that, for $B(x,y)=A(x+y,y)$ (Section 3.1),

$$[T^{n-d}]\frac{P(T)}{(1-T)(1-qT)}(y+xT)^n=\frac{B(x,y)-(x+y)^n}{q-1}. \tag{10}$$

We recall the following properties of the zeta polynomial from [3]. Let $A(x,y)$ be the weight enumerator of a code with q^k codewords and let $g=n+1-k-d$. Let the dual code have $g^\perp=n+1-k^\perp-d^\perp$.

$$\deg P(T)=g+g^\perp=n+2-d-d^\perp, \tag{11}$$

$$P(1)=1, \tag{12}$$

$$P^\perp(T)=P(1/qT)q^gT^{g+g^\perp}. \tag{13}$$

The properties hold for a general linear code.

4.1. General linear codes

For $p(x,y)=y(y-(q-1)x)$,

$$p(x,y)(D)(y(1-T)+xT)^n=n(n-1)(1-T)(1-qT)(y(1-T)+xT)^{n-2}.$$

Define

$$(\nabla A)(x,y)=\frac{1}{n(n-1)}\,p(x,y)(D)A(x,y).$$

Applying $p(x,y)(D)$ to both sides of (9) and dividing by $n(n-1)$ gives

$$[T^{n-d}]P(T)(y+(x-y)T)^{n-2}=\frac{\nabla A(x,y)}{q-1}$$

or, with $P(T)=\sum p_iT^i$,

$$\sum p_i\binom{n-2}{d-2+i}(x-y)^{n-d-i}y^{d-2+i}=\frac{\nabla A(x,y)}{q-1}. \tag{14}$$

Similarly, for $q(x,y)=(y-x)(y-qx)$,

$$q(x,y)(D)(y+xT)^n=n(n-1)(1-T)(1-qT)(y+xT)^{n-2}.$$

Define

$$(\nabla B)(x,y)=\frac{1}{n(n-1)}\,q(x,y)(D)B(x,y).$$

Applying $q(x,y)(D)$ to both sides of (10) and dividing by $n(n-1)$ gives

$$[T^{n-d}]P(T)(y+xT)^{n-2}=\frac{\nabla B(x,y)}{q-1}.$$

And

$$\sum p_i\binom{n-2}{d-2+i}x^{n-d-i}y^{d-2+i}=\frac{\nabla B(x,y)}{q-1}. \tag{15}$$

A code has dual distance $d^\perp$ if and only if $x^{d^\perp-2}$ is the highest power of x that divides $\nabla B(x,y)$. It follows that $\deg P(T)=(n-d)-(d^\perp-2)=n+2-d-d^\perp$ (11). Also, with Theorem 14, a code is MDS if and only if $\nabla B(x,y)=(q-1)\binom{n-2}{d-2}y^{d-2}x^{d^\perp-2}$ if and only if $P(T)=1$.

Lemma 16. *For a linear code of length n and minimum distance d and dual minimum distance $d^\perp$ with weight enumerator $A(x,y)$, let $P(T)$ be the zeta polynomial. Then*

$$T^{d-2}\sum_{i=0}^{n+2-d-d^\perp}p_i\binom{n-2}{d-2+i}T^i=\frac{(\nabla A)(1+T,T)}{q-1}=\frac{(\nabla B)(1,T)}{q-1}.$$

Proof. Substitute $x=1+T, y=T$ in (14) and $x=1, y=T$ in (15). □

4.2. Type 1 codes

For divisible codes we define $(\nabla A)(x,y)$ in a different way that matches with Theorem 3. For $p(x,y)=y(y^c-(q-1)^cx^c)$,

$$p(x,y)(D)(y(1-T)+xT)^n=(n-c)_{c+1}\,p(T,1-T)(y(1-T)+xT)^{n-c-1}.$$

Define

$$(\nabla A)(x,y)=\frac{1}{(n-c)_{c+1}}\,p(x,y)(D)A(x,y)$$

and let

$$Q(T)=P(T)\frac{p(T,1-T)}{(1-T)(1-qT)}.$$

Lemma 17. *For a Type* 1 *divisible code, and for* $p(x,y)$, ∇A *and* $Q(T)$ *as above*

$$\text{(Type 1)}\quad [T^{n-d}]Q(T)(y+(x-y)T)^{n-c-1}=\frac{(\nabla A)(x,y)}{q-1}. \tag{16}$$

In general, the left-hand side equals

$$\sum_{i=0}^{n+2-d-d^{\perp}+c-1} q_i \binom{n-c-1}{d-c-1+i}(x-y)^{n-d-i}y^{d-c-1+i}.$$

For an extremal divisible weight enumerator of Type 1, *the right-hand side equals*

$$(d-c)_{c+1}A_d/(q-1)(n-c)_{c+1}y^{d-c-1}(x^c-y^c)^{d^{\perp}-c-1}.$$

Proof. Apply $p(x,y)(D)$ to both sides of (9) and divide by $(n-c)_{c+1}$. The left-hand side is obvious, the right-hand side uses Theorem 3. □

4.3. Type 2 codes

For $p(x,y)=xy(y^c-x^c)$,

$$p(x,y)(D)(y(1-T)+xT)^n=(n-c-1)_{c+2}\,p(T,1-T)(y(1-T)+xT)^{n-c-2}.$$

Define

$$(\nabla A)(x,y)=\frac{1}{(n-c-1)_{c+2}}\,p(x,y)(D)A(x,y)$$

and let

$$Q(T)T=P(T)\frac{p(T,1-T)}{(1-T)(1-2T)}.$$

Lemma 18. *For a Type* 2 *divisible code, and for* $p(x,y)$, ∇A *and* $Q(T)$ *as above*

$$\text{(Type 2)}\quad [T^{n-d-1}]Q(T)(y+(x-y)T)^{n-c-2}=\frac{(\nabla A)(x,y)}{q-1}. \tag{17}$$

In general, the left-hand side equals

$$\sum_{i=0}^{n+2-d-d^{\perp}+c-2} q_i \binom{n-c-2}{d-c-1+i}(x-y)^{n-d-1-i}y^{d-c-1+i}.$$

For an extremal divisible weight enumerator of Type 2, *the right-hand side equals*

$$(n-d)(d-c)_{c+1}A_d/(n-c-1)_{c+2}(xy)^{d-c-1}(x^c-y^c)^{d^\perp-c-1}.$$

Proof. Apply $p(x,y)(D)$ to both sides of (9) and divide by $(n-c-1)_{c+2}$. The left-hand side is obvious, the right-hand side uses Theorem 3. □

4.4. Extremal self-dual codes

Analogues of Lemmas 17 and 18 for all extremal self-dual codes are obtained easily with Theorem 12. Let parameters m and v be defined for each type as follows:

$$\text{(Type I)} \quad n-4=4(d-3)+2v=4m+2v, \quad v=0,1,2,3,$$

$$\text{(Type II)} \quad n-6=6(d-5)+8v=6m+8v, \quad v=0,1,2,$$

$$\text{(Type III)} \quad n-4=4(d-4)+4v=4m+4v, \quad v=0,1,2,$$

$$\text{(Type IV)} \quad n-3=3(d-3)+2v=3m+2v, \quad v=0,1,2.$$

Note that the extremal codes of Types III and IV are of Type 1. And that the codes of Types I and II are of Type 2. Using the corresponding definitions for $p(x,y)$ and $Q(T)$ gives

$$\text{(Type I)} \quad Q(T)=P(T),$$

$$\text{(Type II)} \quad Q(T)=P(T)(1-2T+2T^2),$$

$$\text{(Type III)} \quad Q(T)=P(T)(1+3T^2),$$

$$\text{(Type IV)} \quad Q(T)=P(T)(1+2T).$$

Theorem 19. *For an extremal divisible code with weight enumerator* $A(x,y)$, *and for* $Q(T)$ *as defined above*:

$$\text{(Type I)} \quad \sum_{i=0}^{2m+2v} q_i \binom{4m+2v}{m+i} (x-y)^{3m+2v-i} y^{m+i} = C(xy)^m(x^2-y^2)^m(x^2+y^2)^v,$$

$$\text{(Type II)} \quad \sum_{i=0}^{4m+8v} q_i \binom{6m+8v}{m+i} (x-y)^{5m+8v-i} y^{m+i} = C(xy)^m(x^4-y^4)^m(x^8+14x^4y^4+y^8)^v,$$

$$\text{(Type III)}\quad \sum_{i=0}^{2m+4v} q_i \binom{4m+4v}{m+i} (x-y)^{3m+4v-i} y^{m+i} = Cy^m(x^3-y^3)^m(x^4+8xy^3)^v,$$

$$\text{(Type IV)}\quad \sum_{i=0}^{m+2v} q_i \binom{3m+2v}{m+i} (x-y)^{2m+2v-i} y^{m+i} = Cy^m(x^2-y^2)^m(x^2+3y^2)^v,$$

where

$$\text{(Type III)–(Type IV)}\quad C=(d-c)_{c+1}A_d/(q-1)(n-c)_{c+1},$$

$$\text{(Type I)–(Type II)}\quad C=(n-d)(d-c)_{c+1}A_d/(n-c-1)_{c+2}.$$

Proof. The left-hand side uses Lemmas 17 and 18. The right-hand side uses Theorem 12. □

The expressions simplify further when dividing both sides by y^m followed by the substitution $x=1+T, y=T$. In particular for an extremal Type IV code with $v=0$,

$$\sum_{i=0}^{m} q_i \binom{3m}{m+i} T^i = C(1+2T)^m. \tag{18}$$

5. A class of self-reciprocal polynomials

We seek to recover the polynomial $Q(T)$ from a description such as Eq. (18), and more generally from descriptions such as in Theorem 19. Consider a self-reciprocal polynomial $R(T)=\sum_{i=0}^{v} r_i T^i$ that satisfies, for some λ,

$$\sum_{i=0}^{v} r_i \binom{v+2\lambda-2}{\lambda-1+i} T^i = (1+T)^v. \tag{19}$$

With hindsight, we claim that

$$\binom{v+2\lambda-2}{\lambda-1} R(T^2) = \frac{v!T^v}{(\lambda)_v} C_v^\lambda\left(\frac{T+T^{-1}}{2}\right), \tag{20}$$

where C_v^λ is an ultraspherical polynomial of degree v. As we mentioned in Section 1.3, for each $\lambda > -1/2$, ultraspherical polynomials form a family of orthogonal polynomials on the interval $[-1,1]$. Using the following expression for C_v^λ [12] the verification reduces to a straightforward comparison of coefficients.

$$C_v^\lambda\left(\frac{T+T^{-1}}{2}\right) = \sum_{\substack{0\leqslant k,l\leqslant n\\ k+l=n}} \binom{k+\lambda-1}{k}\binom{l+\lambda-1}{l}\frac{T^{k-l}+T^{l-k}}{2}. \tag{21}$$

Another proof using results from [2] is included in Section 5.3. For the polynomial $Q(T)$ in (18) we have $Q(T)=R(2T)$ for $v=m$ and $\lambda=m+1$. It follows that $Q(T)$ has all its zeros of the form $2T=e^{2i\theta}$ for real θ, in other words all zeros lie on the circle of radius $\frac{1}{2}$.

For $v=2g$ even, we will generalize to the case where the right-hand side of (19) is an arbitrary self-reciprocal polynomial. For $v=2g$, the cosine polynomial of C_v^λ has constant term $\binom{g+\lambda-1}{g}^2$. Dividing throughout by this factor yields

$$\binom{2g+2\lambda-2}{g+\lambda-1} R(T^2)=T^{2g}\binom{2g}{g} C_{2g}^\lambda\left(\frac{T+T^{-1}}{2}\right)\Big/\binom{g+\lambda-1}{g}^2.$$

Consider now

$$\sum_{i=0}^{2g} r_i \binom{2g+2\lambda-2}{\lambda-1+i} T^i = T^j(1+T)^{2g-2j}, \tag{22}$$

which equals the previous equation when $j=0$. The index i in the left sum can be taken from $i=j$ to $2g-j$ and after a substitution $i=j+k$,

$$\sum_{k=0}^{2g-2j} r_{j+k}\binom{2g-2j+2\lambda+2j-2}{\lambda+j-1+k} T^k=(1+T)^{2g-2j}.$$

For the polynomial $R_j(T)=\sum r_{j+k}T^k$, we find

$$\binom{2g+2\lambda-2}{g+\lambda-1} R_j(T^2)$$
$$= T^{2g-2j}\binom{2g-2j}{g-j} C_{2g-2j}^{\lambda+j}\left(\frac{T+T^{-1}}{2}\right)\Big/\binom{g+\lambda-1}{g-j}^2.$$

Theorem 20. *Let* $R(T)=\sum_{i=0}^{2g} r_iT^i$ *satisfy, for some* λ,

$$\sum_{i=0}^{2g} r_i\binom{2g+2\lambda-2}{\lambda-1+i} T^{2i}=T^{2g}\sum_{j=0}^{g}\alpha_j(T+T^{-1})^{2j}\Big/\binom{2j}{j}.$$

Then

$$\binom{2g+2\lambda-2}{g+\lambda-1}\sum_{i=0}^{2g} r_iT^{2i}=T^{2g}\sum_{j=0}^{g}\alpha_j\tilde{C}_{2j}^{g+\lambda-j}\left(\frac{T+T^{-1}}{2}\right)$$

for the normalization

$$\tilde{C}_{2j}^{g+\lambda-j}\left(\frac{T+T^{-1}}{2}\right)=C_{2j}^{g+\lambda-j}\left(\frac{T+T^{-1}}{2}\right)\Big/\binom{g+\lambda-1}{j}^2.$$

Proof. For a term in the right-hand side

$$T^{2g}\alpha_j(T^{-1}+T)^{2j}\Big/\binom{2j}{j}=T^{2g-2j}\alpha_j(1+T^2)^{2j}\Big/\binom{2j}{j}.$$

And (22) applies with $T=T^2$ and the change of variable $j\mapsto g-j$. The contribution of the jth term to $R(T^2)$ is $R_j(T^2)T^{2j}$. And $R(T)$ is given by

$$R(T)=\sum_j \alpha_j R_{g-j}(T^2)\Big/\binom{2j}{j}. \qquad \square$$

The expansion of $(T+T^{-1})^{2j}/\binom{2j}{j}$ gives the cosine polynomial of $(\cos\theta)^{2j}$ normalized such that the constant coefficient equals 1. Thus, recovering $R(T)$ may be described in two steps as (1) develop the right-hand sum as a sum of normalized cosine powers and (2) replace the cosine powers by normalized ultraspherical polynomials.

5.1. Application to self-dual codes

For a self-dual linear code of length n and minimum distance d with weight enumerator $A(x,y)$, let $P(T)$ be the zeta polynomial and let $g=n+1-k-d=n/2+1-d$. Then, Lemma 16 gives

$$\sum_{i=0}^{2g} p_i\binom{n-2}{d-2+i}T^i=\frac{1}{T^{d-2}}\,\frac{\nabla A(1+T,T)}{q-1}=\frac{1}{T^{d-2}}\,\frac{\nabla B(1,T)}{q-1}.$$

For a self-dual code $R(T)=P(T/\sqrt{q})$ is self-reciprocal. And Theorem 20 applies with $\lambda=d-1$ and $2g=n+2-2d$.

Lemma 21. *For a self-dual weight enumerator $A(x,y)$ with zeta polynomial $P(T)$, let*

$$\frac{1}{T^{d-2}}\,\frac{\nabla A(1+T,T)}{q-1}=q^gT^{2g}\sum_{j=0}^{g}\alpha_j(\sqrt{q}T+\sqrt{q}^{-1}T^{-1})^{2j}\Big/\binom{2j}{j}.$$

Then, for $R(T)=P(T/\sqrt{q})$,

$$\binom{n-2}{n/2-1}\sum_{i=0}^{2g}r_iT^{2i}=T^{2g}\sum_{j=0}^{g}\alpha_j\tilde{C}_{2j}^{n/2-j}\left(\frac{T+T^{-1}}{2}\right).$$

For codes with small coefficients α_j when j is small, the dominant term $C_{2g}^{n/2-g}=C_{2g}^{d-1}$ will give an approximation for the zeta polynomial $P(T)$. The coefficients α_j are linear in the coefficients A_i of the weight enumerator and can thus be estimated using linear programming.

5.2. Application to extremal self-dual codes

For the extremal self-dual codes with $v=0$, we obtain from Theorem 19

$$\text{(Type I)}\quad \sum_{i=0}^{2m} q_i \binom{4m}{m+i} T^i = C(1+3T+2T^2)^m,$$

$$\text{(Type II)}\quad \sum_{i=0}^{4m} q_i \binom{6m}{m+i} T^i = C((1+3T+2T^2)(1+2T+2T^2))^m,$$

$$\text{(Type III)}\quad \sum_{i=0}^{2m} q_i \binom{4m}{m+i} T^i = C(1+3T+3T^2)^m,$$

$$\text{(Type IV)}\quad \sum_{i=0}^{m} q_i \binom{3m}{m+i} T^i = C(1+2T)^m.$$

In each of the following cases, Theorem 20 applies to $R(T)=Q(T/\sqrt{q})$. With the previous expressions, the coefficients α_j become

$$\text{(Type I)}\quad \alpha_j = C\binom{2j}{j}\binom{m}{j}(3\sqrt{2}/2-2)^{m-j} \quad (g=m, \lambda=m+1),$$

$$\text{(Type II)}\quad \alpha_j = C\binom{2j}{j}\sum_{k+l=j}\binom{m}{k}\binom{m}{l}(3\sqrt{2}/2-2)^{m-k}(\sqrt{2}-2)^{m-l} \quad (g=2m, \lambda=m+1),$$

$$\text{(Type III)}\quad \alpha_j = C\binom{2j}{j}\binom{m}{j}(\sqrt{3}-2)^{m-j} \quad (g=m, \lambda=m+1).$$

For (Type IV) codes, we find directly

$$\text{(Type IV)}\quad Q(T^2/2)C'T^m C_m^{m+1}\left(\frac{T^{-1}+T}{2}\right).$$

In all cases, the coefficients α_j are small when j is small, and the function $R(T)$ can be approximated by neglecting terms with small j.

5.3. Zeros of hypergeometric functions

We express the polynomial $R(T)$ in (19) as a hypergeometric polynomial. And we show a relation with the class of polynomials $F(-v,\lambda;2\lambda;w)$ that was studied in [2]. In that paper, the expression

$$F(-v,\lambda;2\lambda;1-T^2) = \frac{v!\,T^v}{(2\lambda)_v} C_v^{\lambda}\left(\frac{T+T^{-1}}{2}\right) \tag{23}$$

is used to show that the hypergeometric polynomial $F(-v,\lambda;2\lambda;w)$ has all its zeros of the form $w=1-e^{2i\theta}$, for some real θ. The relation with $R(T)$ is clear by comparison of (23) and (20). For the coefficients of $R(T)$, we have

$$r_0\binom{v+2\lambda-2}{\lambda-1}=1$$

and, for $i>0$,

$$r_{i+1}=r_i\left(\frac{n-i}{i+1}\right)\left(\frac{n+\lambda-1-i}{\lambda+i}\right)=r_i\left(\frac{-n+i}{i+1}\right)\left(\frac{-n-\lambda+1+i}{\lambda+i}\right).$$

Comparison with the definition of a hypergeometric series

$$F(a,b;c;x)=\sum_{i=0}^{\infty}\frac{(a)_i(b)_i}{(c)_i}\frac{x^i}{i!}$$

shows that

$$\binom{v+2\lambda-2}{\lambda-1}R(T)=F(-v,\lambda;-v-\lambda+1;T). \tag{24}$$

Now

$$F(-v,\lambda;2\lambda;1-T)=\frac{(\lambda)_v}{(2\lambda)_v}F(-v,\lambda;-v-\lambda+1;T) \tag{25}$$

and combining (24), (25), and (23) we obtain

$$\binom{v+2\lambda-2}{\lambda-1}R(T^2)=\frac{(2\lambda)_v}{(\lambda)_v}\frac{v!\,T^v}{(2\lambda)_v}C_v^{\lambda}\left(\frac{T+T^{-1}}{2}\right).$$

Eq. (21) that was used above follows from (23) and

$$F(-v,b;2b;1-w)=\frac{1}{(2b)_n}\sum_{k=0}^{n}\binom{n}{k}(b)_k(b)_{n-k}w^k. \tag{26}$$

Eqs. (23), (25) and (26) are from [2].

6. Conclusion

Theorem 12 gives expressions for extremal self-dual weight enumerators that can be used to considerably shorten proofs for some of their properties. The theorem yields explicit expressions for the zeta functions of extremal self-dual weight enumerators which in principle allows us to verify that these functions have their zeros on a circle, as conjectured in [5]. For codes of type IV this is immediate. For the codes of types I, II, III this appears to be the case but a detailed proof is lacking. Another open problem is to estimate, through linear programming methods, the coefficients in the expansion of a zeta function as a sum of ultraspherical polynomials.

Acknowledgements

I am indebted to Kenneth Stolarsky for valuable comments and for pointing out Ref. [2].

References

[1] A. Ashikhmin, A. Barg, Binomial moments of the distance distribution: bounds and applications, IEEE Trans. Inform. Theory 45(2) (1999) 438–452.
[2] K. Driver, P. Duren, Zeros of the hypergeometric polynomials $F(-n,b;2b;z)$, Indag. Math. (N.S.) 11(1) (2000) 43–51.
[3] I.M. Duursma, Weight distributions of geometric Goppa codes, Trans. Amer. Math. Soc. 351(9) (1999) 3609–3639.
[4] I.M. Duursma, From weight enumerators to zeta functions, Discrete Appl. Math. 111(1–2) (2001) 55–73.
[5] I.M. Duursma, A Riemann hypothesis analogue for self-dual codes, in: A. Barg, S. Litsyn (Eds.), Codes and Association Schemes (Piscataway, NJ, 1999), American Mathematical Society, Providence, RI, 2001, pp. 115–124.
[6] I. Krasikov, S. Litsyn, An improved upper bound on the minimum distance of doubly-even self-dual codes, IEEE Trans. Inform. Theory 46(1) (2000) 274–278.
[7] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, Vol. 16, North-Holland, Amsterdam, North-Holland Mathematical Library, 1977.
[8] C.L. Mallows, N.J.A. Sloane, An upper bound for self-dual codes, Inform. Control 22 (1973) 188–200.
[9] E.M. Rains, Shadow bounds for self-dual codes, IEEE Trans. Inform. Theory 44(1) (1998) 134–139.
[10] E.M. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman, R.A. Brualdi (Eds.), Handbook of Coding Theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 177–294.
[11] N.J.A. Sloane, Self-dual codes and lattices, in: Relations Between Combinatorics and Other parts of Mathematics (Proceedings of Symposium on Pure Mathematics, Ohio State University, Columbus, OH, 1978), American Mathematical Society, Providence, RI, 1979, pp. 273–308.
[12] G. Szegő, Orthogonal Polynomials, Vol. XXIII, American Mathematical Society, 4th Edition, Colloquium Publications, Providence, RI, 1975.
[13] H.N. Ward, Divisible codes, Arch. Math. (Basel) 36(6) (1981) 485–494.
[14] S. Zhang, On the nonexistence of extremal self-dual codes, Discrete Appl. Math. 91(1–3) (1999) 277–286.